Multimedia fingerprinting with noise via signature codes for weighted noisy adder channels and compressed sensing

Elena Egorova[1], Marcel Fernandez[2], and Moon Ho Lee[3]

[1] Skolkovo Institute of Science and Technology (Skoltech), Moscow region, Russia
elena.egorova@skolkovotech.ru
[2] Universitat Politcnica de Catalunya, Barcelona, Spain
marcel@entel.upc.edu
[3] Division of of Electronics, Chonbuk National University, Republic of Korea
moonho@jbnu.ac.kr

Abstract. We propose a new coding scheme for multimedia fingerprinting resistant to noise. Our scheme is based on signature codes for weighted noisy adder channel. The scheme (codes) can trace the entire coalition of pirates and provides significantly better rate than previously known fingerprinting schemes. We also establish a relationship between these two problems and the compressed sensing problem.

1 Introduction

There are the following well established concepts of digital fingerprinting codes known as *tracing traitors* [1] or *codes with the identifiable parent property* [2], and *digital fingerprinting codes* [3],[4], dealing with the problem of protection against unauthorized copying of discrete data. A theoretical model for data protection of continuous data was proposed in [5] and [6]. The corresponding codes, called *multimedia fingerprinting codes*, were investigated in [5] - [11]. First multimedia fingerprinting codes with nonvanishing rate, namely with the rate of order t^{-2}, where t is the coalition's size, were constructed in our paper [12]. Generalizations of results from [12] to the case of presence of noise was done in [13]. All previous considerations of multimedia fingerprinting codes were based on some discretisation, introduced in [5], i.e., only *hard decoding* of such codes was investigated. In this paper we consider the output of the corresponding channel without discretisation, i.e. we consider *soft decoding* of multimedia fingerprinting codes. We show that the corresponding model of multimedia fingerprinting channel without discretisation is equivalent to some modification of some model of the adder channel, considered in [14], which we call *weighted adder channel*. And signature codes for

the weighted real adder channel can be considered as multimedia fingerprinting codes with soft decoding. We show that the rate of multimedia fingerprinting codes with soft decoding is at least $1/t$ what is much larger than for the hard decoding which rate cannot exceed $O(t^{-2}\log t)$ even for the noiseless case, see [12].

2 Channel model of multimedia fingerprinting

Consider, following [5], [6], multimedia content being represented as a real-valued vector $\mathbf{x} \in R^m$, called the host signal. To prevent unauthorized redistribution of $\mathbf{x}$, the dealer constructs a set of digital fingerprints using a linear modulation scheme that employs n *noise-like* orthonormal signals (vectors) $\{\mathbf{f}_i \in R^m \mid i = 1, \ldots, n,\ n \leq m\}$. The fingerprint $\mathbf{w}_j$ of the $j-$th user ($j \in \{1, \ldots, M\}$) is represented as follows:

$$\mathbf{w}_j = \sum_{i=1}^{n} h_{ij}\mathbf{f}_i, \tag{1}$$

where $h_{ij} \in \{+1, -1\}$ if for antipodal signals and $h_{ij} \in \{0, 1\}$ for on-off keying type of modulation. Below we consider the case on-off keying type of modulation. The sets of fingerprints $\{\mathbf{w}_j\}$ will be called a fingerprinting code. Equivalently and more convenient is to consider the set of n-dimensional binary vectors $\mathbf{h}_j = (h_{1j}, \ldots, h_{nj})$ as binary multimedia fingerprinting code of length n, cardinality M and rate $R = n^{-1}\log_2 M$.

The dealer distributes to the j-th user the vector

$$\mathbf{y}_j = \mathbf{x} + \mathbf{w}_j,$$

where one assumes that $\|\mathbf{x}\|_2 \gg \|\mathbf{w}_j\|_2$ in order to be sure that the fingerprinting scheme do not introduce significant changes in the host signal.
A group of users, called *colluders* or *pirates*, aims to create an unauthorized copy of the contents such that the dealer cannot trace its origins to any of them. An important concept in digital fingerprinting, the *Marking Assumption* of [3], in the context of multimedia fingerprinting can be expressed in the following way: we *assume* that the members of the pirate coalition $J \subset \{1, \ldots, M\}$ cannot manipulate individual signals $\mathbf{f}_j$, and are limited to *linear attacks*. By a linear attack we mean that pirates can generate a forged copy $\hat{\mathbf{y}}$ of the host content only as a linear combination

of their copies $\mathbf{y}_j$ with some coefficients λ_j

$$\hat{\mathbf{y}} = \sum_{j \in J} \lambda_j \mathbf{y}_j \tag{2}$$

where $\lambda_j > 0$ for all j and $\sum_{j \in J} \lambda_j = 1$. Hence

$$\hat{\mathbf{y}} = \mathbf{x} + \sum_{j \in J} \lambda_j \mathbf{w}_j. \tag{3}$$

The dealer calculates the vector $\mathbf{S} = \mathbf{S}(J, \{\lambda_j\}) = (s_1, \ldots, s_n)$, where

$$s_k = (\widehat{\mathbf{y}} - \mathbf{x}, \mathbf{f}_k) = \langle \sum_{i=1}^{n} \sum_{j \in J} \lambda_j h_{ij} \mathbf{f}_i, \mathbf{f}_k \rangle = \sum_{j \in J} \lambda_j h_{kj} \tag{4}$$

and $\langle \cdot, \cdot \rangle$ denotes the inner product. Equivalently,

$$\mathbf{S} = \sum_{j \in J} \lambda_j \mathbf{h}_j, \tag{5}$$

where $\mathbf{h}_j = (h_{1j}, \ldots, h_{nj})$. It was suggested in [5], [6] to consider the following discretisation, when the dealer knows only whether $s_k = 0$, or $s_k = 1$, or that $0 < s_k < 1$, but does not know the value of s_k in the last case. Note, that $s_k = 0$ means that $h_{kj} = 0$ for all $j \in J$, $s_k = 1$ means that $h_{kj} = 1$ for all $j \in J$ and finally $0 < s_k < 1$ means that

$$\{\cup_{j \in J} h_{kj}\} = \{0, 1\} \tag{6}$$

It means that the dealer observes ternary output, i.e., the output of the 2-frequency noiseless multiple-access channel without intensity information [15] (the A-channel, for short), see more detailed explanation in the next section. This approach to constructing multimedia fingerprinting codes as signature codes for the A-channel was developed in [12].

In almost all previous works on multimedia fingerprinting codes it was assumed that the dealer observes the forged copy $\hat{\mathbf{y}}$ *without noise*. This simplified assumption is not very realistic. Indeed, there are at least two sources of noise: a measurement noise, and a malicious noise, produced by the coalition. Therefore we assume that the dealer observes the following vector as a result of coalition forgery

$$\mathbf{z} = \mathbf{x} + \sum_{j \in J} \lambda_j \mathbf{w}_j + \mathbf{E}, \tag{7}$$

where $\mathbf{E} = (E_1, \ldots, E_m)$ and let for simplicity E_i be i.i.d.r.v. Similarly to (4) and (5) the dealer evaluates

$$s_k(\mathbf{E}) = (\widehat{\mathbf{z}} - \mathbf{x}, \mathbf{f}_k)$$

and the following vector

$$\mathbf{S}(\mathbf{E}) = (s_1(\mathbf{E}), \ldots, s_n(\mathbf{E})) = \sum_{j \in J} \lambda_j \mathbf{h}_j + \mathbf{e}, \tag{8}$$

where $\mathbf{e} = (e_1, \ldots, e_n)$ and $e_k = \langle \mathbf{E}, \mathbf{f}_k \rangle$. Based on the known value of the vector $\mathbf{S}(\mathbf{E})$ the dealer tries to reveal (to trace) the whole coalition, which produced this forgery, or at least one of its members. We shall consider $\mathbf{S}(\mathbf{E})$ as the output of *continuous* multimedia fingerprinting channel which is in fact a modification of well known adder channel with noise. We call this channel as *weighted adder channel*. Indeed, equation (8) with $\lambda_j \equiv 1$ and $\mathbf{e} = \mathbf{0}$ describes the output of the adder channel with binary input in the case of t active users among M, and λ_j plays the role of weights. We show that multimedia fingerprinting codes capable to trace the whole coalition of size t are in fact the same as t-signature code for the weighted adder channel, and the number of users M equals to the cardinality of the corresponding signature code. Note that an intermediate case of the weighted adder channel $\lambda_j > 0$ was firstly considered in [14] (where weights λ_j were called gains) but consideration of noise was restricted in [14] to the very particular case $\mathbf{e} = b\mathbf{1}$, where b is a real number. Finally, we establish a relationship between the weighted adder channel and the compressed sensing problem [16],[17].

3 Codes for noiseless weighted adder channel

Recall that the dealer observes the output of the following multiple-access channel, which we called the weighted adder channel (WAC, for short), see (8), with unknown weights λ_j and unknown set J of active users of WAC,i.e., the set of traitors. The dealer goal is to find the set J, what corresponds to zero-error coding for multiple-access channel (MAC) with partial activity, i.e. not all possible users of MAC are active, but not more than t of them. We shall consider the set of n-dimensional binary vectors $\mathbf{h}_j = (h_{1j}, \ldots, h_{nj})$ as a binary multimedia fingerprinting code of cardinality M capable to find any set of t or less traitors in the

case of s noiseless WAC iff for any subsets $J, J' \subset \{1, \ldots, M\}$ such that $|J| \leq t,\ |J'| \leq t$ the following equality

$$\sum_{j \in J} \lambda_j \mathbf{h}_j = \sum_{j \in J'} \lambda'_j \mathbf{h}_j \tag{9}$$

implies that $J = J'$ (and $\lambda_j = \lambda'_j$ for all j).

It's easy to see that this condition is equivalent to the linear independence (over real numbers) of any $2t$ vectors $\mathbf{h}_j$. Such effective set of vectors is well known in coding theory as columns of a parity-check matrix of a binary BCH code of length M and redundancy n, correcting t errors. Indeed, any $2t$ columns are linear independent over the field of residues by module 2, and hence they are independent over the rational numbers and also over the real numbers since in all cases dependency means that the determinant of the corresponding $t \times t$ minor equals to 0. It is not clear if this construction is even weakly optimal, i.e., has the minimal possible order of n as a function of M - for binary BCH-codes it gives $n = t \log_2 M(1 + o(1))$. Anyway we see that in the case of absence of quantization, i.e. soft decision, the rate of the best multimedia fingerprinting code is at least $1/t$ whereas for hard decoding the rate of any multimedia fingerprinting code is $O(t^{-2} \log t)$ [12].

4 Codes for noisy weighted adder channel and the compressed sensing problem

Now we want to construct codes which are capable to recover a set J by its "syndrom" $\mathbf{S}(\mathbf{E}) = \sum_{j \in J} \lambda_j \mathbf{h}_j + \mathbf{e}$, see equation (8).
It is very similar to the compressed sensing problem, see [16],[17], with the only three differences:
for "weakly" multimedia fingerprinting code it is sufficient to find at least one $j \in J$ for sure;
for multimedia fingerprinting we need to find only the "error" set J, and solution of compressed sending problem means to find J and values λ_j;
vectors $\mathbf{h}_j$ are *binary*.

Consider slightly other statement of the problem, more in the spirit of coding theory, namley, that the number of errors is limited, i.e., $wt(\mathbf{e}) \leq T$. A solution of this problem was given in [18], see also [19]. If to omit details (which can be found in [18]) then in order to correct T syndrom's errors one should "add" $T \log(t \log M)$ redundant symbols what gives the total redundancy $n = t \log_2 M + T \log_2 \log_2 M + T \log_2 t$. It is easy to

check that for $T - const$ it keeps the same order of rate, namely $R = t^{-1}(1 + o(1))$. Note that a similar technique was used in [20].

5 Conclusion

Let us note in conclusion that the problem of noise in multiple-access channels was almost ignored probably because of the following remark in [15] "A more sophisticated model taking such errors into account could easily be developed. One method would be to use a noisy channel in cascade with our noiseless channel. It is our contention, however, that although the details are different, the basic ideas are the same in the noisy and noiseless cases." Our construction is much better than such simple cascade.

Acknowledments

The work of M. Fernández has been supported by the Spanish Government through projects Consolider Ingenio 2010 CSD2007-00004 "ARES," and TEC2015-68734-R (MINECO/FEDER) "ANFORA."

References

1. B.Chor, A.Fiat, and M.Naor. "Tracing traitors". *Advances in Cryptology-Crypto'94, LNCS*, 839, pp. 480–491, 1994.
2. H. D. L. Hollmann, J. H. van Lint, J.-P. Linnartz, and L. M. G. M. Tolhuizen, "On codes with the Identifiable Parent Property," *J. Combinatorial Theory, Ser. A*, vol. 82, no. 2, pp. 121–133, May 1998.
3. D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.
4. G. Tardos, "Optimal probabilistic fingerprint codes." in *Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA*, ACM, 2003, pp. 116–125.
5. W. Trappe , M. Wu ,Z.J. Wang ,K.J.R. Liu , "Anti-collusion fingerprinting for multimedia", *IEEE Trans. Signal Process.* vol. 51, pp. 1069-1087, 2003.
6. K.J.R. Liu, W. Trappe, Z.J.Wang, M. Wu and H.Zhao. Multimedia fingerprinting forensics for traitor tracing. Vol. 4. Hindawi Publishing Corporation, 2005.
7. M.Cheng and Y.Miao, "On Anti-Collusion Codes and Detection Algrithms for Multimedia Fingerprinting". *IEEE Trans. Info. Theory*, vol. 57, no. 7, pp. 4843-4851, 2011.
8. M.Cheng, L. Ji and Y.Miao, "Separable Codes", *IEEE Trans. Info. Theory*, vol. 58, no. 3, pp. 1791-1803, 2012.
9. Fei Gao and Gennian Ge, "New bounds on separable codes for multimedia fingerprinting", *IEEE Trans. Info. Theory*, vol. 60, pp. 5257-5262, 2014.

10. M.Cheng, H-L Fu, J. Jiang, Y-H Lo and Y.Miao, "New bounds on 2-separable codes of length 2", *Designs, Codes, and Cryptography*, vol. 74, no. 3, pp. 31-40, 2015.
11. Jiang, J., Cheng, M., Miao, Y., "Strongly separable codes". Designs, Codes and Cryptography, 79(2), pp. 303-318, 2016.
12. E. Egorova, M. Fernandez, G. Kabatiansky, and Moon Ho Lee, "Signature codes for A-channel and collusion-secure multimedia fingerprinting codes", Proceedings 2016 IEEE International Symposium on Information Theory, Barcelona, pp. 3043-3047, 2016.
13. E. Egorova, M. Fernandez and G. Kabatiansky, "Multimedia Fingerprinting Codes Resistant Against Colluders and Noise", Proceedings of 8th IEEE International Workshop on Information Forensic and Security, Abu Dhabi, pp. 1-5, 2016.
14. P.Mathys, "A Class of Codes for a T Active Users Out of N Multiple-Access Communvation System", *IEEE Trans. Info. Theory*, vol. 36, No 6, pp. 1206-1219, 1990.
15. Chang S. C., Wolf J. K., "On the T-user M-frequency noiseless multiple-access channel with and without intensity information", *IEEE Trans. Inform. Theory* vol. 27, no. 1, pp. 41-48, 1981.
16. D. L. Donoho, "Compressed sensing", *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1289-1306, 2006
17. E. J. Candes, T. Tao, "Near-Optimal Signal Recovery From Random Projections: Universal Encoding Strategies? ", *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 5406 - 5425, 2006
18. Kabatiansky, G., Lomakov, V., Vladuts, S. "On codes correcting errors in channel and syndrom", Problems of Information Transmission, v.51, N.2, pp. 50-57, 2015.
19. Kabatiansky G., Vladuts S., Tavernier C., "On the Doubly Sparse Compressed Sensing Problem", IMAAC 2015, *LNCS*, vol. 9496, pp. 1-6, 2015.
20. Gritsenko V., Kabatiansky G., Lebedev V. and Maevskiy A., "Signature codes for noisy multiple access adder channel", Designs, Codes and Cryptography, 82(1), pp. 293-299, 2017.